Claims

WHAT IS CLAIMED IS:

1. A method to remotely validate an email message, comprising:
receiving the email message in a first encrypted format;
decrypting the email message from the first encrypted format;
transferring the decrypted email message to a remote server; and
receiving from the remote server a status flag, wherein a value associated with the status flag indicates whether the email message is validated by the remote server.

2. The method of claim 1, further comprising encrypting the email message in a second encrypted format before transferring the email message to the remote server.

3. The method of claim 1, further comprising accessing the email message for use, if the value of the status flag indicates the remote server validated the email message.

4. The method of claim 1, wherein in transferring the email message, the first encrypted format is a Secure Multi-Purpose Internet Mail Extension (S/MIME) format.

5. The method of claim 1, wherein in receiving the status flag, if the value of the status flag indicates the remote server validated the email message, then subsequent accesses made to the email message do not result in the email message being transferred to the remote server for validation.

6. The method of claim 1, wherein in transferring the email message, the email message is streamed to the remote server.

7. A method to validate a data message, comprising:

receiving the data message from a client;

scanning the data message for viruses; and

sending a validation flag to the client, wherein the validation flag includes a value indicating whether the data message includes zero or more of the viruses.

8. The method of claim 7, further comprising decrypting the data message before scanning the data message.

9. The method of claim 8, wherein in decrypting the data message, the data message is decrypted using a public key of the client.

10. The method of claim 7, wherein in receiving the data message, the data message is an email message and the client is an email client.

11. The method of claim 7, wherein in receiving the data message, the data message is received from an operating system residing on the client.

12. The method of claim 7, wherein in scanning the data message, a scanning set of executable instructions is selectively executed to scan the data message for zero or more of the viruses.

13. The method of claim 7, wherein in receiving the data message, the data message is received as a data stream from the client and scanned as the data stream is received.

14. An email system to validate an email message, comprising:

a local email set of executable instructions residing on a client;

a remote validation set of executable instructions residing on a server; and

wherein the email message is received by the local email set of executable instructions, decrypted, and streamed to the remote validation set of executable instructions wherein the email message is scanned and a validation flag associated with a result of the scan is sent to the local email set of executable instructions.

15. The email system of claim 14, wherein the local email set of executable instructions accesses the email message if the result indicates the scan validated the email message.

16. The email system of claim 15, wherein the scan validates the email message if the email messages is free of viruses.

17. The email system of claim 14, wherein the local email set of executable instructions removes the data message if the result indicates the scan did not validate the email message.

18. The email system of claim 14, wherein communications between the local email set of executable instructions and the remote validation set of executable instructions are secure.

19. The email system of claim 18, wherein public and private key pairs associated with the client and the server are used to encrypt and authenticate the communications.

20. The email system of claim 14, wherein the email message includes an attachment message and wherein the email message is in a Secure Multi-Purpose Internet Mail Extension (S/MIME) format when received by the local email set of

executable instructions.

21. An email message residing on a computer readable medium operable to be remotely validated, comprising:

a first encrypted format associated with content data of the email message, wherein an email client decrypts the first encrypted format to render the content data; and

a second encrypted format associated with the content data, wherein the email client generates the second encrypted format, and wherein the email client transfers the second encrypted format to a remote server where the content data is rendered by the remote server by decrypting the second encrypted format, and wherein the remote server scans the content data for viruses.

22. The email message of claim 21, wherein a validation flag indicating whether zero or more of the viruses are detected in the content data is generated by the remote server and sent to the email client.

23. The email message of claim 21, wherein the first encrypted format is a Secure Multi-Purpose Internet Mail Extension (S/MIME) format.

24. The email message of claim 21, wherein the second encrypted format is generated by using a private key for the email client and a public key for the remote server.

25. The email message of claim 21, wherein the email client accesses the content data for use when the remote server detects no viruses.

26. The email message file of claim 21, wherein the content data includes text data and attachment data.